

(designated in accordance with section E.3.a., DoD Directive 5200.1,³⁹ or their representatives) responsible for directing and administering the Information Security Program of the OJCS, the Departments of the Army, Navy, and Air Force, the Defense Intelligence Agency, the Defense Nuclear Agency, the National Security Agency, and the Defense Investigative Service. Other DoD Components may be invited to attend meetings of particular interest to them.

Subpart O—Administrative Sanctions

§ 159a.97 Individual responsibility.

All personnel, civilian or military, of the Department of Defense are responsible individually for complying with the provisions of this part.

§ 159a.98 Violations subject to sanctions.

(a) DoD Military and civilian personnel are subject to administrative sanctions if they:

(1) Knowingly and willfully classify or continue the classification of information in violation of E.O. 12356, any implementing issuances, or this part.

(2) Knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under E.O. 12356 or prior orders; or

(3) Knowingly and willfully violate any other provision of E.O. 12356, any implementing issuances or this part.

(b) Sanctions include but are not limited to a warning notice, reprimand, termination of classification authority, suspension without pay, forfeiture of pay, removal or discharge, and will be imposed upon any person, regardless of office or level of employment, who is responsible for a violation specified under this paragraph as determined appropriate under applicable law and DoD regulations. Nothing in this part prohibits or limits action under the Uniform Code of Military Justice based upon violations of that Code.

§ 159a.99 Corrective action.

The Secretary of Defense, the Secretaries of the Military Departments,

and the heads of other DoD Components shall ensure that appropriate and prompt corrective action is taken whenever a violation under § 159a.98(a) occurs or repeated administrative discrepancies or repeated disregard of requirements of this Regulation occur (see § 159a.100). Commanders and supervisors, in consultation with appropriate legal counsel, shall utilize all appropriate criminal, civil, and administrative enforcement remedies against employees who violate the law and security requirements as set forth in this part and other pertinent DoD issuances.

§ 159a.100 Administrative discrepancies.

Repeated administrative discrepancies in the marking and handling of classified information and material such as failure to show classification authority; failure to apply internal classification markings; failure to adhere to the requirements of this part that pertain to dissemination, storage, accountability, and destruction, and that are determined not to constitute a violation under § 159a.98(a) may be grounds for adverse administrative action including warning, admonition, reprimand or termination of classification authority as determined appropriate under applicable policies and procedures.

§ 159a.101 Reporting violations.

(a) Whenever a violation under § 159a.98(a)(2) occurs, the Director of Counterintelligence and Investigative Programs, ODUSD(P) shall be informed of the date and general nature of the occurrence including the relevant parts of this part, the sanctions imposed, and the corrective action taken. Whenever a violation under § 159a.98(a) (1) or (3) occurs, the Director of Security Plans and Programs, OSUSD(P) shall be provided the same information. Notification of such violations shall be furnished to the Director of the ISOO in accordance with § 5.4(d) of E.O. 12356 by the ODUSD(P).

(b) Any action resulting in unauthorized disclosure of properly classified information that constitutes a violation of the criminal statutes and evidence reflected in classified information of

³⁹ See footnote 1 to § 159a.3